REMARKS

In the Office Action dated September 14, 2006, the Examiner allowed claims 1-10 and 24 and rejected claims 12-23 under 35 U.S.C. § 103(a) as being unpatentable over Subramaniam in view of Steiner et al., hereinafter Steiner. The Applicant would like to thank the Examiner for the indication of allowable subject matter in claims 1-10 and 24, and respectfully requests the Examiner reconsider the rejection of claims 12-23 in light of the following remarks.

The present invention is directed to flaws associated with the Kerberos security protocol system typically used for a single user. The Kerberos system for authenticating a user in an application-level protocol does not work for Windows 95 and 98 environments because the file system is not secure enough and multiple users are not allowed. The present invention proposes a system that uses Kerberos-based principles to allow multiple users to communicate securely through their firewalls to reach remote applications.

Independent claims 12 and 23 of the present invention are directed to a method for accessing a service by a user in which a user ticket and sequence number are presented to a service through a web adapter. The service is chosen within the service server. A session name, encrypted with the ticket and user identification is sent to a privilege server and a session key and sequence number are requested. The session name is received from the user; the user ticket and a user privilege are validated. When the user is validated, a session key and sequence number are issued for the ticket. The session key and sequence number are encrypted with the ticket to form a packet, and the packet and ticket are sent to the service.

The privilege server is an important part of the present invention and the authentication process is far more detailed than validation of a username and password. The policy engine of the privilege server is the main component of the privilege server and interacts with various functional blocks of the system,

most importantly for issuing a ticket or sequence number for a user. The privilege server allows the possibility of connecting to multiple proxy servers.

The Examiner asserted that independent claims 12, 13 and 23 were unpatentable over Subramaniam in view of Steiner. It is respectfully asserted that the present invention is patentable over the Subramaniam and Steiner reference. The Steiner reference is directed to the Kerberos method and the present invention is directed to a method and system that applies Kerberos-based principles to a method for accessing a service by a user. The Subramaniam method is directed to securing intranet access in a way that is very different than the present invention. It is respectfully asserted that there is no suggestion or motivation for applying Kerberos-based principles to the teachings of the Subramaniam reference. It is also respectfully asserted that even if the references were combined as suggested by the Examiner, their combination would not result in the Applicants' invention.

The Subramaniam reference is directed to secure intranet access to provide secure access to a network from an external client. The present invention also provides secure access to a service available on an external network, but does so in a very different way than the teachings of the Subramaniam reference. The Subramaniam reference teaches an external client requests access to data which is stored on a target server. The IP address of the requesting client is checked to determine if the request came from outside the security parameter. Upon that determination, the target server redirects the request to a border server. The user is authenticated and validated by a software database. Once access is granted, the signal is changed from HTTP to HTTPS thereby forming a secure connection between the external client and the border server. According to the teachings of Subramaniam, there would be no need for presenting a user ticket, sending a session name encrypted with the ticket and encrypting the session key and sequence number for the ticket before sending the

packet and the ticket to the requested service as taught in the method and system of the present invention. The use of "https" in Subramaniam, a client cannot connect to a second proxy/headend server and have services rendered with a single sing-on feature.

Because Subramaniam teaches the redirection of a request and the formation of a secure connection between the border server and the external client through the use of "https" protocol, it cannot possibly teach or suggest the method claimed by the present invention. Because Subramaniam presents a method for secure intranet access by identifying a user from a database and modifying URL's to make them secure once access is granted. There is no need for encrypted tickets, tokens and the like in the method taught by Subramaniam. It is respectfully asserted that there is inherently no motivation to combine the teachings of the Subramaniam reference with Kerberos-based principles.

Furthermore, it is asserted that even if combined with the teachings of Steiner, which explains the Kerberos method, the combination would not result in the applicant's invention. It has been asserted above that Subramaniam does not teach or disclose a privilege server as taught by the present invention. The Examiner points to Figure 1, number 140 and column 8, lines 47 to column 9 line 10 of Subramaniam as teaching a privilege server. However, it is respectfully asserted that Subramaniam is merely disclosing a software database for rejecting or validating authentication of a user and in no way teaches or discloses a privilege server that is capable of applying the principles applied in the present invention. In the present invention the privilege server is part of the authentication system and has a policy engine therein, this is neither taught nor disclosed in Subramanaim. The privilege server 26 of the present invention contains the policy engine 28 and is coupled to the user 12 who is external to the authentication system 10 of the present invention. The privilege server of the present invention contains the policy engine which is coupled directly to various

functional blocks that interact with data being either sent to the user or received from the user. The policy engine also interacts with the key generator to issue the ticket or sequence number for a user and decides which services of which components should be used in a sequence. The policy engine is formed by the privilege server. This is neither taught nor disclosed in Subramaniam.

It is respectfully asserted that the software database taught in the Subramaniam reference cannot be considered equivalent to a privilege server as claimed in the present invention. Therefore, it is respectfully asserted that even if the Subramaniam reference were combined with the Steiner reference, the combination would not result in the applicant's invention which requires a privilege server that validates the user and issues a sequence number and session key encrypted with the ticket to form a packet. The packet is sent to the service and the user is validated by receiving the packet from the web adapter. Even if the teachings of Subramaniam were combined with Keberos-based principles, the software database 140 of Subramaniam would be incapable of handling the functions of the privilege server taught in the present invention and the combination of Subramaniam and Steiner would require significant modifications to accomplish results similar to the authentication system and method of the present invention.

Regarding independent system claim 13, the Examiner indicated that the Subramaniam reference teaches a privilege server coupled to an intermediate server in Figure 1, reference number 140 and at column 8-9. It is respectfully asserted that the software 140 that identifies the username and user password as taught in Subramaniam is not the same as the privilege server of the present invention. The directory services database 140 as taught in the Subramaniam reference is exclusively for the purpose of authenticating and validating a user. It does not teach or suggest capabilities necessary for applying Kerberos-based principles to authentication of the user.

As discussed with reference to claims 12 and 23, the security aspect taught in the Subramaniam reference lies in changing the protocol from HTTP to HTTPS. There is no need for generating and encrypting tickets or tokens. It is respectfully asserted that there is no motivation to combine the directory 140 of Subramaniam with Kerberos-based principles because the security of the network as taught in Subramaniam is directly related to the modification of URL's once a user has been validated. Therefore, it is respectfully asserted that one skilled in the art would not look to combine Subramaniam with Kerberos-based principles as suggested by the Examiner because there is no need for a privilege server to apply the generation of tickets and tokens, as claimed in the present invention, to the teachings of the Subramaniam reference. And as explained above, even if the references were combined as suggested by the Examiner, the Subramaniam reference, the Steiner reference, and there combination lack any teachings of a privilege server that is capable of handling the extensive functions necessary to accomplish the authentication method and system taught in the present invention. Even if Subramaniam were combined with Steiner their combination would not result in a system that allows a client to connect to multiple proxy servers.

It is respectfully requested the Examiner reconsider the rejection of the present application in light of the amendments and remarks herein to withdraw the rejection of claims 12-23 and issue a formal Notice of Allowance for claims 1-10 and 12-24. Should the Examiner remain unconvinced by the present response, it is respectfully requested that he contact the undersigned in order to discuss any possible amendments to the claims that may bring them into condition for allowance.

Respectfully submitted,

Angela M. Brunetti
Reg. No. 41,647

Attorney for Applicant(s)

Date: December 14, 2006

Artz & Artz, P.C.
28333 Telegraph Road, Ste. 250
Southfield, MI 48034
Tel: 248-223-9500
Fax: 248-223-9522